2017 年 5 月 12 日，星期五

一周威胁综述（5 月 5 日至 5 月 12 日）

本文概括介绍 Talos 在 5 月 5 日至 5 月 12 日观察到的最常见威胁。与之前的威胁聚焦一样，本文不进行深入分析，而是重点从以下方面总结我们观察到的威胁：关键行为特征、危害表现，以及我们的客户是如何自动得到保护、免受这些威胁的。

在此提醒，本文中介绍的关于以下威胁的信息并不十分详尽，但所述内容截至发稿日期为止为最新。对以下威胁的检测和防护会根据进一步的威胁或漏洞分析进行更新。如需获取最新信息，请参阅 FireSIGHT 管理中心、Snort.org 或 ClamAV.net。

本周最常见的威胁包括：

- **Doc.Downloader.WithMacro-6310867-0**
  Office 宏下载程序
  这是一个混淆的 Office 宏下载程序，最终会利用 Powershell 下载恶意的负载可执行文件。典型对象交互通过 WITH 命令进行混淆。

- **Heuristics.W32.Parite.B**
  病毒
  Parite.B 是一个多态文件感染程序。它可以感染本地计算机和网络驱动器上的可执行文件。

- **Js.Downloader.Nemucod-6311824-1**
  基于脚本的下载程序
  Nemucod 是一个基于 JS 的下载程序，这种下载程序向来是多种垃圾邮件攻击活动和猖獗的漏洞攻击包十分惯用的方式，通常作为在受感染主机上植入常见勒索软件的一个阶段。该特定变种非常依赖十六进制字符连接 ∓ 命名规范，包括随机的 0、o 或 0 字符。

- **Pdf.Tool.HeapSprayHeuristic-6301967-1**
  PDF JS 堆喷射
  PDF 通过嵌入的 JavaScript 利用漏洞，或者至少获得对 JavaScript 提供的其他功能的访问权限。典型的漏洞利用技术需要堆喷射，使用 JavaScript 在整个进程内存中多次复制相同的数据。

- **Win.Dropper.Elex-6310653-0**
  植入程序
  这是一个使用 powershell 脚本从 dga 域下载文件的 dll。我们观察到安装的广告插件为 Elex，但也可以是其他插件。此 dll 还包含在原始驱动器上执行操作的指示器。它通过服务安装确保持续感染系统。

- **Win.Trojan.Generic-6305879-0**
  蠕虫
  Gamarue 是一种通过可移动驱动器、垃圾邮件和漏洞攻击包传播的蠕虫。它与多个恶意域进行通信，可用于在受感染计算机上安装其他恶意软件。

- **Win.Trojan.Nanocore-5**
  RAT
  Nanocore 是一种 .NET 远程管理木马。它的源码已泄露多次，使得它广泛可用。与其他 RAT 一样，它可让攻击者完全控制系统，包括录制视频和音频、窃取密码和文件记录按键等。

威胁

Doc.Downloader.WithMacro-6310867-0

危害表现

注册表项
- 不适用

互斥体
- 不适用

IP 地址
- 185[.]165[.]29[.]36

域名
- 不适用

创建的文件和/或目录
- 不适用

文件散列值
- 009ea577f9f7c8d311b96051c3a6e4fe288647fe4122c2fb0c14240565097012
- 015f06d82006879a5e040e913f8ea91ed5ad01249f753cfbf1888daeb19073e3
- 01dba2caf8c50e171d4cfb45b788b589af06f4a467174325c88f200ca7ca9198
- 0212c580c27761eddea2af38b0a0c1fb9b32789c5574ea7a23f8184570d8dfb6
- 03aaf18f3a59fb063622511d6b441999ff90c06742911419052251ec320146b8
- 040e61e10a7a85c23041c1f0e4635dd2ea9307787eb17e88f80372529e9209d5
- 06e4b3a33127ddd8ff0157fc0ba1d2d24a8f26ed1a149b4388c01d30350c0ccb
- 072e99a20f62ec2d713db7e088edac0fcdb90a77f0b10aacd7d0e549d694f0ed
- 0a428729361a8a712cbfd3d8574b234306c12c32b327d3cd207fa188460b1e3f
- 0a7922eb74e6139a08fa8735a87cc47fc62c1f6325aadbac2bc82c2981f2ada1
- 0b9e0425aea9565b0307a322976f77edc6802e443cf5f62f724fec4ad83a9d28
- 0bacdef1c789dde9662570062587098b7c693bb7be89c0a22b824aa5fbff6056
- 0bfc71f69f2bd4db2ae9fc900e11509852e1eb8874f39171287e86bb7284868e

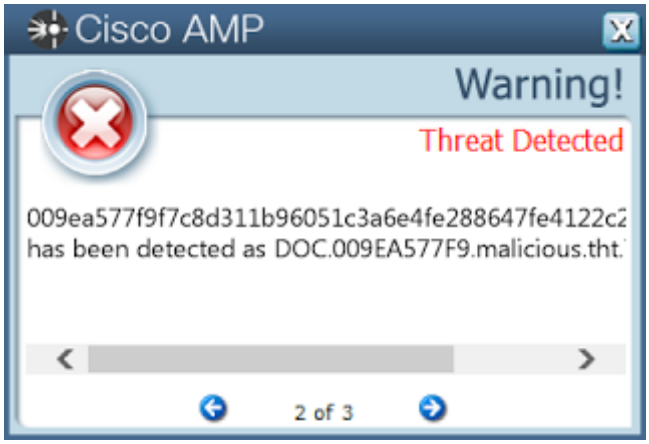
- 0c7f5c69e828c88778314be34c3468ab9a2bc9705cba727bb3c89832c3f91113
- 0e9246ff490f54d156cc3426e434980bb98a81935f1c9666a93237428b8e0ea0
- 11769cdaf3c210df174702803fbc4afa7b2cc20a27ec30ed0e4f81118a66de10
- 11fe367d79f104632d9452027a7377b4c51fc0f43f32d7a6fe73f34fc2cce508
- 11feca2c6b6d0be07e01bbaa910ef8a44c81f89ad1dabcdc5eeddb37ff12d854
- 12e7c347609f1b2aea12e47f12d15df579c22162a49338977d4694dad7fff028
- 1333e3e5be8cc510e33c609a7080764b12cab70e5ddbb57167309f15557edcae
- 14cc6de1dd265d0943a96b4852e6f8c5828f636131333d0c19b2dc5f7a0ca1ff
- 15bafa0d6de0681cd079ae866c4ed4f1c9917ce96261215564c8f0029f9675e8
- 177477fcf8963dbef8e22bd32f7f08e4b103af89ba7f3e7a4a997513e1532629
- 17abb7ca3e200e5c7965ffee65629d3d113717bd858377948e577200e6be11b7
- 1997e3d6ba77ea68160b88c083aca9bca8d8bbf8e1191e86c1660f7a4b038f93
- 19d6fc360c1af923e44f173989591f382ab965767802bc54a2df875a10ca4e38
- 1a50f4767495978a5ca9e34fcde61a74657e04d12b04bac60c0b0b6aac26c588
- 1b6a81db9bf395f8f80e1d23b143d5ac049af16878f66ecd3874f4cda406836a
- 1f9a0e385cbce520988e24bf1b95b4cd7976d46637864e5fb20548068b3cc4eb
- 220791a76a3befad1dd9e71a8664ab7546ee1cc98a9b061abb2cfd577b8bf55b
- 25291ca354bd11e6864e84eee74b3a271541e4aa6e8479f3cafe13210b8bafcf
- 28b343fc742da18b7ffc9a2e5e9c49b8f54cb6ac724849ccb56b4d079088d1c6
- 2a7eae250d89a5fdc9ee3acb57d1f068eb5b1ed06aa48c9093d095c3187271e7
- 2b3ea225733847126 90f76dbc939935a848a739f61a7c69e92f11b4eb77bbc41
- 2c960ecfc9cb060bf73cff44accc258f47164c3b7b497bdf3d02f7088bce7d7d
- 2e0b71ae5e202e569ecfa9731f58376e1d24a5dea725e4ef2eda64939dfba226
- 2f0220eb391f691e51b2afc724d9cd04a9f869e34fe9e8c715e864f13546136e
- 2f0877a8ebbad2f4e11709da5a99453b812a86ba0e5502a6b0791b856fc9dc6c
- 2f571cc5b3f708e3a6da99c9d61f99d0230052e9a0cc483644044f92537a7ddf
- 30224c91115b5c4212de3dcb8cbb412b59084d8bea1ea9f54525de0a07362b68
- 30a37e174b9a8433ca9befda236c985daa5b92aa8cd078e8f6e033e61914caa3
- 31819465f95180892f68afb2f4bda5eaafcb1ac7138fcdd0e91e951eeb307e47
- 33242ab139dfef3cd6f6e2938d54737c5efcdaf00217e1c5b49c2dc5618449ec
- 34ca6fe49ec7c5b318e55183d09c350af5b418209558ca1ff6bdc53034fcaced
- 358782ef63e14ff6606fc4e1b91da61ba19383e403fab6997cf5d2b000d5136d
- 36d1b267808d306d96ff40520b1cd1f04b861847313dd0ea60fb5bf764843b21
- 3736940527681c6c0daf9c25fdc1807868bab9c339a61a7ed88f8c7e335128f3
- 37f39f494673dabdb49c254a02aeca1dd350f8ea828b928cd4d8f42e6c6cd264
- 37fa50440f8950df0d0dbebe2b052925d9014ab85c3c8b62e3d9fa49f327cc41
- 3ab653f63c43209910645d6d87d8b60419ace960dd16e275f407cf46bce0b8b8

防护

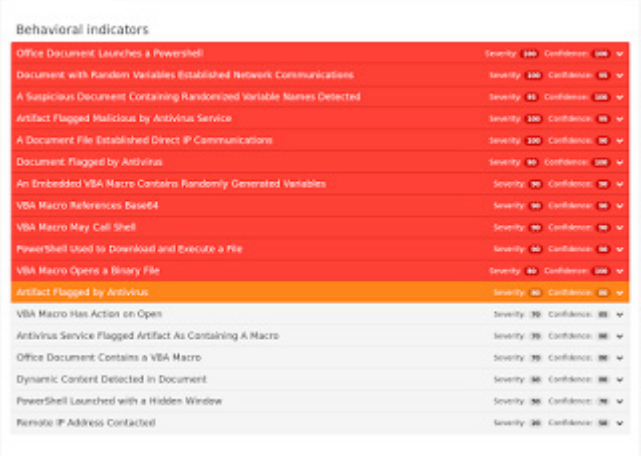
产品	防护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Heuristics.W32.Parite.B

危害表现

注册表项

- 不适用

互斥体

- 驻留

IP 地址

- 不适用

域名

- 不适用

创建的文件和/或目录

- \Documents and Settings\Administrator\Local Settings\Temp\jnj1.tmp
- %SystemDrive%\DOCUME~1\ADMINI~1\LOCALS~1\Temp\mhbD.tmp

文件散列值

- 00667eb42299cf767fd996961e426f3af3471c71f1e612ec2d832576289077d2
- d8e6807fb1b2ca4d3e9ce8c15415839ed8e9a57cfe7d3e362d0e225de436eb77
- 5a16d398170bc582ddc864b35271526defce211dc9026739fdeca9260414f36a
- 742fff7851b87b91583f54c2c70438ede8af603aef3e3897e5792665b382b0bb
- 3107785dfb03aa0a1b072ab4a9de383733cc53724f94d04647129848a2418d79
- 415d459846a0f9453963b0474d6a6ad877c7c25c72e445b0f6e6e585cd5b400e
- 2c4657c53467b77fa8c007468ce756f623e302294a288782041c3fd225828af4
- e67254d17730ec06704cd78f65182380f02f6e09997b2d9fec815d7209705965
- 50ee4a9db6b125b5b57693f2aeb622c3133811f31e6b81034f3bcbec5af7f6f9
- 644d71edbc489214fc98d55504059da222f888169363a5d7d21e44ddf1d825c9

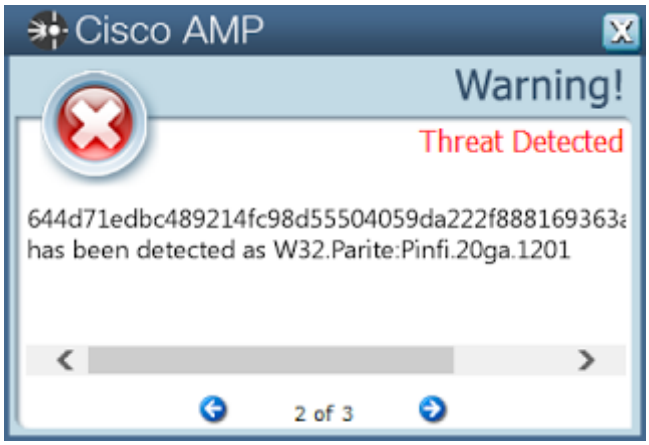
- a176ecdb644b79d68cd721a7b417edb425a88e9cdfec6c490b194056e3a47024
- 8f0419896c6b0dd5bdb2748777f3e96c4bbfb7f7e96ae88fecb025607fa2d194
- 9510fd8c732f0ffd693931090c326ebaf2ba12f2b2c6ea53225d932adfc4bd22
- 0280366ea9ccf3412e0eb354b03c2ddb9ebf5a60eb236a0aa6a4334033b8d267
- d31e56c10e62524c241d878b4ab94eea6193bfcd22f4b89f3fd8beb9c55cc9da
- d2674afebf388fc5b068288df275554b098b8c2ff3bc93606025a273f5c09670
- de0210ad1d7c25c124b110ef3fed6386ff25a311e35ea301d83bf7be9eecc23c
- 23c81c28545fe91270f72dd2463609ecac4ba8163ebadabce343f18425a08929
- 2345aab3ecebc954de2839fd61501f9fa8fb886566f85f88be535ecdbb263d2a
- 0c6478931f2e3edb41d5b6cca8d4f033864a033e084323762a0cc0714b62f128

防护

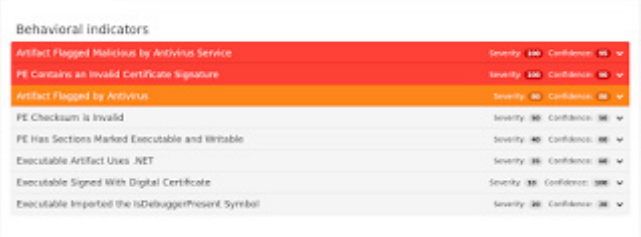
产品	防护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Js.Downloader.Nemucod-6311824-1

危害表现

注册表项

- **HKU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections**

互斥体

- 不适用

IP 地址

- 不适用

域名

- 37kddsserrt[.]pw

创建的文件和/或目录

- 不适用

文件散列值

- 15a37811fe59536bfee4155c41b94911d9d507beaaff2fa673dd1da3e1f369e0
- 1a7e222d39aef7ac4d8006503b46145e127ce6eca82eb75c22163a73c40e27b3
- 20ffb283d1af44cb42afbee43c2b386021e7dedb9c59c1d5a95ac3e05fce9742
- 2f80a68b8603b77c2f138e1a6c082e1308dba1d1e7c7e4d91b25baab67251d0a
- 2f917ae9ce62698dddc07f55bafc3f95937ba2cac1f75e5e2678a1163d175e2c
- 3ba9904b8ebd1b81c406293a55cb1ccac03ef574bbc8f3a2ecaa726930f75b7c
- 441ab6cd707bb4a485395edf30b7b1eff84cc02f2cbd0f6a83c8a269c72c9da7
- 4d8d2444d77fc8c802be80fa93e317316bd86f3f9ee2699d971c89f36a4cbfd3
- 92649f778b58afd71bc8f500465489a67c16be7789f5aff8ffcedb6216679ff2
- 983446fa82305c52ff87a76be94a75ae1c7c10c6c43a6481bd4db8b7e679eddd
- 9c74de5f43b79fd44843126716f8c27b1dc4f33dff779fe2cd7a5eded23c4dd2
- a655770566e3c0783b3fbf8d9be3fb713d9e6380ec3e5a9aef5881f761e8925d
- aec59a27af9c7ca54247666338ad0a6a0d74a23ee0e6bd7c33be76b7872a49ee
- baae74e6a153bb597d8ceb81f22508c55d8697fb748502708c9666d78d53a4c5
- d0f0a5c540a3e68f417590cb4f27a6f9da4401b2b0e71ccabe6f46d0a7e6135f
- d13ffcf550abe6033977d5730babf4dff4358487d35d646c043683515f39e89a

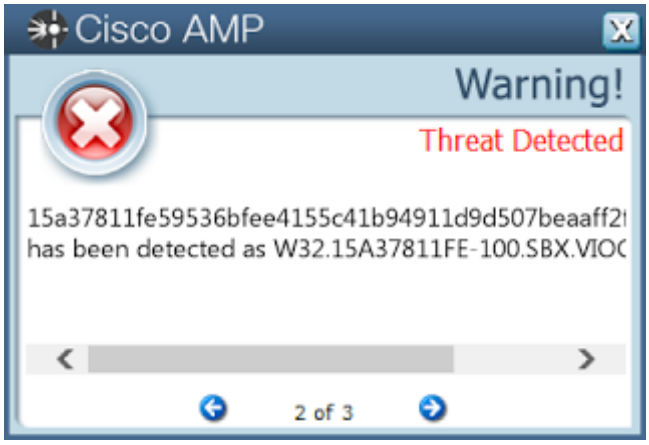
- e290216a1ccb5561d17e1d0d681eb27e7c301d774fdb275fbb1292ba98fa137a
- e4acd53b4ecb0bd3cd0e7a534d4d0a80fd221bbb73c199ffa3f44019a1989a55

防护

产品	防护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	✔
Threat Grid	不适用
Umbrella	✔
WSA	✔

检测结果屏幕截图

AMP



Umbrella

Pdf.Tool.HeapSprayHeuristic-6301967-1

危害表现

注册表项

- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\MPSSVC\PARAMETERS\PORT KEYWORDS\DHCP**
  - **值：**Collection
- **<HKLM>\System\Acrobatviewercpp304**

互斥体

- 2AC1A572DB6944B0A65C38C4140AF2F426c714578B0
- 2AC1A572DB6944B0A65C38C4140AF2F426c714574CC
- 2AC1A572DB6944B0A65C38C4140AF2F426c71457750
- 2AC1A572DB6944B0A65C38C4140AF2F426c71457468
- 2AC1A572DB6944B0A65C38C4140AF2F426c714574A4
- 2AC1A572DB6944B0A65C38C4140AF2F426c71457490
- 2AC1A572DB6944B0A65C38C4140AF2F426c71457828

IP 地址

- 85[.]13[.]129[.]180

域名

- www[.]osterkirchengemeinde[.]de
- www[.]evangelisch-in-rath[.]de

创建的文件和/或目录

- 不适用

文件散列值

- 0ed5bb2ef055843c083d2316999e99827a4ff8bbc143c88a38cc413f9c2c116e
- 4cabe4eaf54b986b6f2170be4e89d98aed85c4012d64c8b4de0f1a74260228de
- 9c85ae448c23c19b4049e5290453027f81681348a28b5f3859aad247855db881
- afaaa1de8842a8e4d57c856cfa48d8eaef4177ba0842431c5108eb65e8b028f1
- 1ef663a739551ca8e3b13ec5d174025a020ca0a9973ebf161532518a4d8c757f
- 706672cad725b4e660d5c5d49d07ac40ecda3f063ba206bf1631ef70e1677b2d
- 0a943757893342c4fa59b3f27b7d5495be02b19c748880fce980e17573ca3603
- 4675f673f32f990cdd142485944cf45578aa44777905ff4f69b79bfca478f78d
- 97dd140d08ad59d23511cd8c693e228c1873f980082a03bc7e6882ec66286cda
- 95e247c1d3e2c57e290333a3d3ddca9d4ec10df89c65a7b2bf6dcf3a149d5707
- b74b8beb8461f677edd2c3668cd2b1b75e10a4ad478dd3f5ab6e0e0ce411173d
- fee4c7f0f121a24026274b75b230e8320153ca6b04398d62e727992dc7805cbf
- 6269e027e2e35a3cc05683a26be9d3912b71821aed363ccfe03fd6714ba62bf9
- 87d75c307f059c7c6b9dae22aa672eee59cbba102fb836157daa4022f4aa2daf
- e708eeff27d67902a1bf69fb5e915b3387e8f978aec3381564bf216614f7fdb2
- 10258a93f571c695996c68ed138af3cfe27599d972ece06d8ff83c41d8feea55
- 22418e0da375bbd39ee22a31b439d943331fbf93090656e0228ba090a5411ced
- 19c8b5e940dd58be7d922b82803551f33edfdd5b99b51f975572672355afac24
- 4c357d0e23b940794e4fd02db568b791d4bbafc3c01f13fed36746c3a8ff7389
- 5246ba3e5adf83a61d531b71010ee97ce95bb0f576de2e5f17d9d9335bf60b5f
- 94a7a438d7583a89eb1c2d36a2c425d2bcebb46da9003881ca56aff7693db25d
- 78d4ccaa8d70737c6c414e22f2fffbdc4f50ce2669d355cfc306e9765041c49d
- 774b078fb180647b85b054f1402b593b418f46cea143ec78bfee33b8549d77eb
- 6b54c11ba12507c70f28b1217ac12b7ffac7565269e49679358e4a6171e0b09d
- e40981cc4fb3302bba6843222c7e2bec31128aed4307247a228656d09362640d
- fb5cb1b158ac996ff9e2181eec27f5e165ee15b7210dc3aa7e1386dbe3fb4c02
- ec87f2b3b3e506e4b56f6b07b6e5287b6907fe692957990581bd5855361f6548
- f211816b7459d3f032cf816f8d218117b19d2b3936b7496e7d7f8ba25745a5a9
- 3d84331388d5ff3bfcafbe9ac21342530028e6697e186a8f2aaeeb91dca07ae8
- 2b8bf40b0c7a7a4c17687d997e2382c701a38704c6218e8bbd23132c755144ba
- 35f378fadf4d4a483dd4fedbc381d3409718896c4d77a2844509f1fc54eefc48
- 734a5745a213cea15d8136aa19134a20a128bfc946158ae3f62293e83cbc9be1
- 97f27903b0514a185be1953a4723b41397cefb323895341976e32303a6c40496
- a88324345da77b1bb039aae33cfaa276dbc2a23a9366ff343f7d4cc814ebed10
- a5fc5fbebb46342d1dd34352227bfb14f95bf942a889d48503b0b70a60ade4d4
- c7f9bd64a9ef18d38575a240490bc84e477397d0ceb92a3fd50b3c54c9e54ed6
- de56b4596f74c18f6bf6214ab4e65f77116b310e8a29e7a311068e0d2e213ab2
- cc218b74a0dcee14ef0ef2945e24c3131fc6ec0e686f0ae4d829884914eaf67b
- d19e62d473c5ed40bc68c46cc3a7bebca0b88f7cb030dce05b2e2c9b65bc9cf9
- 1a069aab9f5b2dcf80ba50bcfb2b19384f1dc366e08d2c2e6d93305340cc69e2

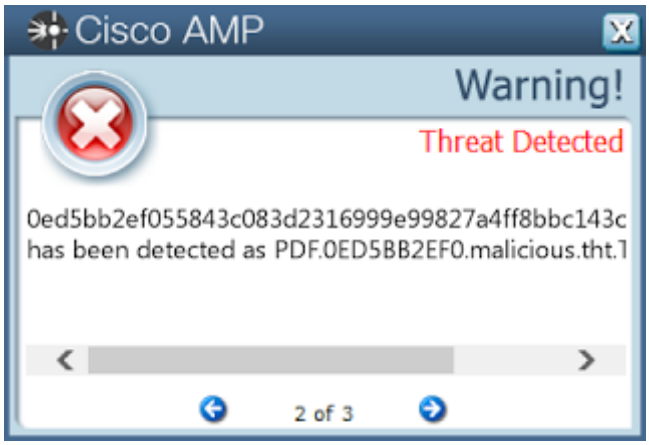
- 1c4e83094a1f5ae3cb209289ea8a88610b54703669537e07acbf329c0b6dcfb1
- 0097500439d1cdfa7201438e2b833ab9aae853d2055be97f555745d22bb4f2dc
- 10e4a16f1dc67f56f2fb8c4e9c77f524dd8e75d3c4da16a310a14655e8f9f350
- 095b45f74868dccbf0c16861d45d664d59207be569a0bbff61dedb6b64995f3d
- 219e6afff26d23e1b86be14ec89573f2c212dbcb825e11fbdbdad4e6788c86b6
- 577ed1dad1ab726daa5fc3a2efdcbd2c737d58c79f9ddd5aa2300876a9b66fc2
- 8e95f4bfd0e6b15b7ebcc5b755419f14fae4acbdf000620be1ed4340259801a7
- aeab75acf64b90cb741e81399ea61f31c86c2ad54ad156c6218f4cfe6b6e3dbf
- 1113a806123f549bcab408286f05f615906bbe93016bb4678899101c533cb4eb
- 1a303ada7458d80307c454c2dc045f169f5623e0b0282ca84ae4682c03ea41a1

防护

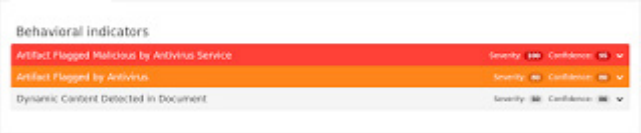
产品	防护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	不适用
Umbrella	不适用
WSA	✔

检测结果屏幕截图

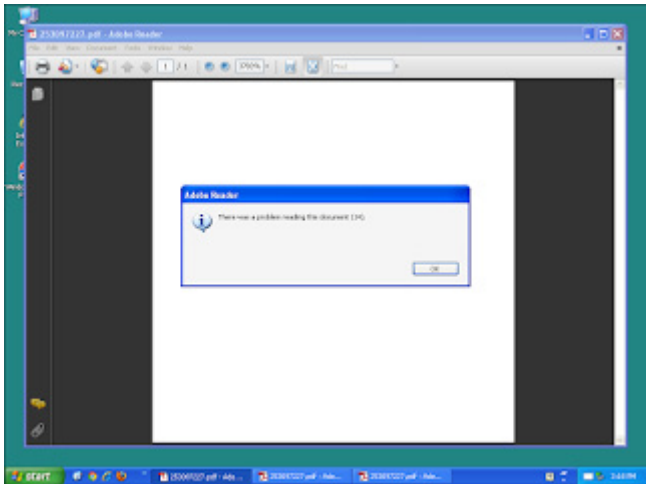
AMP



ThreatGrid



屏幕截图



Win.Dropper.Elex-6310653-0

危害表现

注册表项

- **<HKLM>\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost**
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet**
    - **值：**WinSAPSvc
    - **数据：**参数
- **<HKLM>\SYSTEM\ControlSet001\Services\WinSAPSvc\Parameters**

互斥体

- 不适用

IP 地址

- 不适用

域名

- dhxx2phjrf4w5[.]cloudfront[.]net
- d4c04g24ci6x7[.]cloudfront[.]net
- dc44qjwal3p07[.]cloudfront[.]net
- d3i1asoswufp5k[.]cloudfront[.]net

创建的文件和/或目录

- %AppData%\WinSAPSvc\WinSAP.dll
- %SystemDrive%\winsap_update\Do24_Proxy.exe
- %SystemDrive%\winsap_update\WinSAP.dll
- %SystemDrive%\winsap_update\wsc.dll
- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\cspE.tmp
- %SystemDrive%\winsap_update\winsap_cf

文件散列值

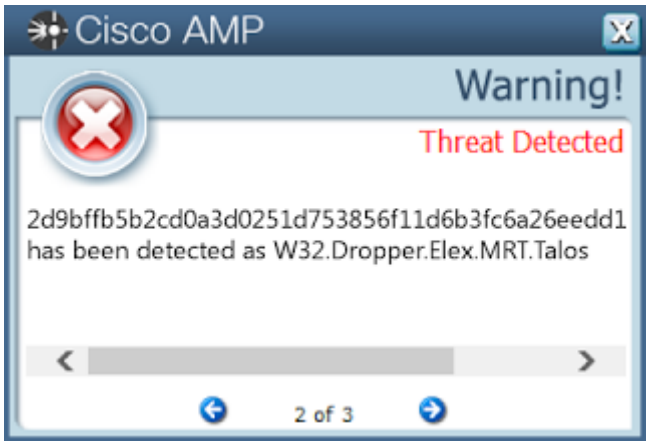
- 9e509317500fbc908cb5cb6a064abcbbf98eeb6ab0825fa5f962ad460674f263
- 540af140928834a0e904d897408e6ceb118aec79835f0050b504541688b028d4
- b00e14ffa5a1995524e938c8c89bfd4f278ffb7e98ef738412cbb0674bc0966a
- 6ffbbfd27387e2a941293ac752b18ef9baa5801f07a3be4695ae465fd8164846
- b1e726e34c0920f8e394af5327f86383ea014d072809f31c409e6d8428629189
- b580b561468763a4ccdd66d37df929fe5b31f615e75dfd8b537eaed1c85213d3
- 632d67e4b439fc0fef2a430b885ada2687e8e0af41c8cf74b37a70e809f7dcde
- 2d9bffb5b2cd0a3d0251d753856f11d6b3fc6a26eedd17c9bbbefe52eafce55b
- c640da31b32d736f784eee0c5adf742cd607388ac3772097b1e4bb184a9839cf
- fd708e0fc599cc3c78f6af9f56af9da466f7f46984d3be5ecc678177a752e027

防护

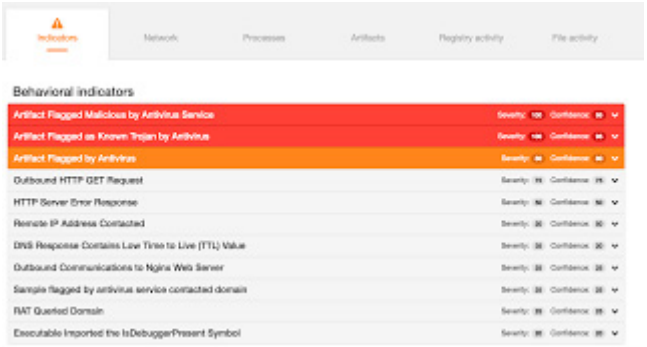
产品	防护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	✔
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Umbrella

Win.Trojan.Generic-6305879-0

危害表现

注册表项

- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**IntranetName
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**AutoDetect
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**IntranetName
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**UNCAsIntranet
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**skypee
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**internat.exe

互斥体

- 4030631218
- lol

IP 地址

- 23[.]253[.]126[.]58
- 166[.]78[.]145[.]90
- 208[.]100[.]26[.]251
- 104[.]239[.]157[.]210
- 65[.]55[.]50[.]189
- 134[.]170[.]58[.]221
- 224[.]0[.]0[.]252
- 192[.]42[.]116[.]41

域名

- imageshells[.]com
- sonic4us[.]ru
- bighecks[.]net
- www[.]yahgodz[.]com

创建的文件和/或目录

- %WinDir%\Skypee\skypee.exe

文件散列值

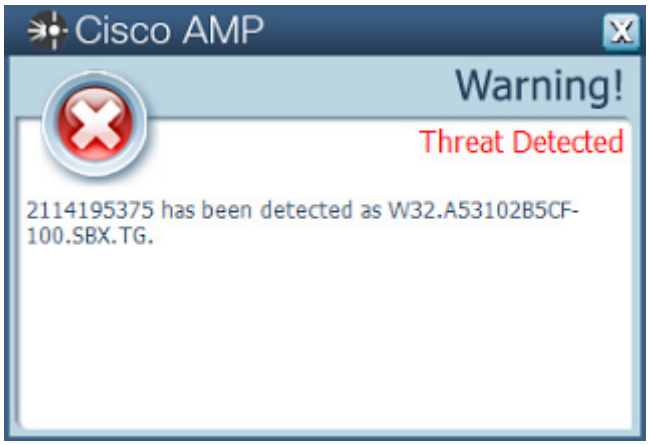
- a53102b5cf8a0d9e395d239b7e3bcd810602d9860a6c013d98eb1260a6e556c1
- ba811b3bdfd1a0a931327fad9ad2c093e18edf17843df225fef862c8092bb67d
- c7b096cbc62fb44ffa9d61cfd829c6ba601996035d91635753cdfd676999bb0b
- 9a62ff51346d88251f6ff3bb06e287adc96f9b25def1ce9fca61b8eae6ceaf31
- 615cc70cdf50d8b217dd54f97d41f58bb3567d9bd49c09bb46d9a945239d9834
- adc844ee16010d8333770d1eb59ced6c15e161ca08a9fd8b3540c16bfd4dde51
- 2219c33bee232930783a85f091d1931b70d079300170699e5b9f3f958d8a504c
- dd3991e7cf0239c99fbebab008cd8e2b4d1748f2506ce52a9dfe89049f84c25d
- d25abadcad1e43d972828f74f6fcc8945d716193c20c966dac04458c56b16cc0
- 7b1e6b8f13e87cdcc61c9924ccd82a9a11e250495261fe65ef9bc0cd658c0cba
- 352485d048b952fb502e967c7504113dcaa65b6bd7d90b4ef1553300c2e1cd10
- bf0a13f37cda4d33191115e22067a70a60ed5e8a47fe64714df6f7c7379229e8

防护

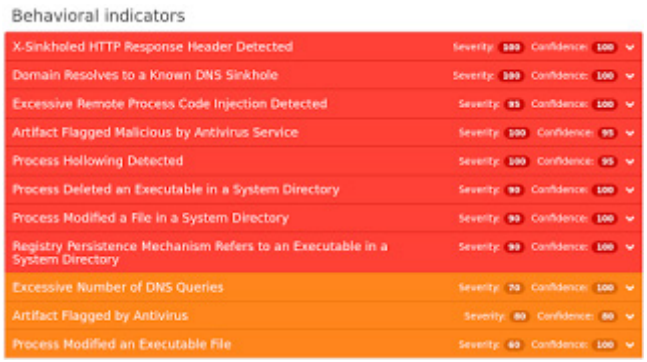
产品	防护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Umbrella

Win.Trojan.Nanocore-5

危害表现

注册表项

- 不适用

互斥体

- 不适用

IP 地址

- 95[.]136[.]188[.]213

域名

- denialfx[.]ddns[.]net

创建的文件和/或目录

- 不适用

文件散列值

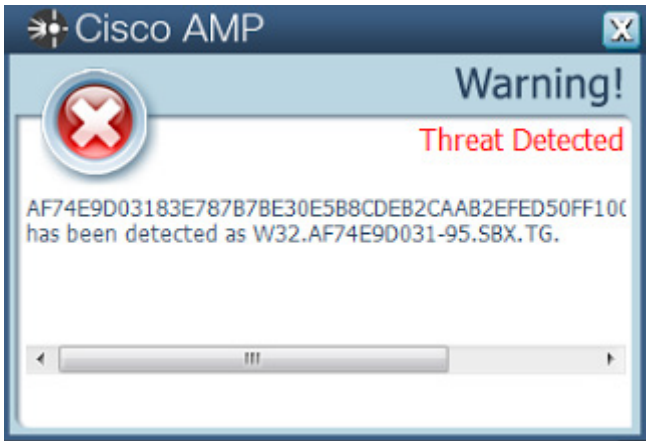
- af74e9d03183e787b7be30e5b8cdeb2caab2efed50ff100b783fa718f5091f17
- 1092399e3f24750b7dcc6bad8ab83011ad36dfb96b0d7096d5589a1c7aeab4f3
- 1b672136fb4aed1cf243d8a60e5f16f22cb7419e3b5bc874d572e1b64e714e9c
- 0d798d302878b8f8860ca469239d18dbe41e6df7fe3e6643783eeb4c8a2f8f84
- 58592983390f2aec8659a7d3750bb11c236fa747408b96e9ec00558c4d7783d8
- aee3bb0f4210c2821c379ba88f06070debef705a3cf14ba3f20a25f9e69d57bc
- 5a08c426b6741e3ecea4b46120f4aaa231aa3718c51e0c026a5a6811b75ee2ca
- 8738e8f913de386cc8e38acab178d73778a2e7e6fb9b9d93654cc965be5d4d2c
- 3e77823a066203d327fe020185852b38d6c7aecf28fa84907cd31d897a3ddb6d
- 9f1c2a1a9068fb232fd072f8c02b88c70303f53f1d816a42902263d2f4ee8103
- 93b627ee36e381a3fe557fc3ac43e5734bcec288a1b96ab84c77c6565ead8c18

防护

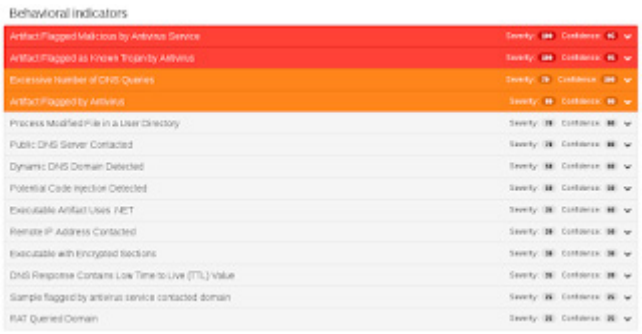
产品	防护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

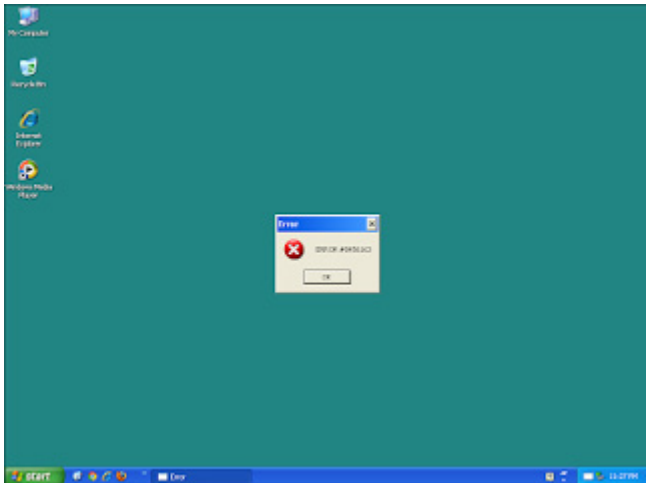
AMP



ThreatGrid



屏幕截图



发布者：ALEXANDER CHIU；发布时间：0:40
标签：AMP、CLAMAV、防护、SNORT 规则、THREATGRID、UMBRELLA